STRATEGY RESEARCH PROJECT

WIELDING THE CYBER SWORD: EXPLOITING THE POWER OF INFORMATION OPERATIONS

BY

LIEUTENANT COLONEL RANDAL A. DRAGON
United States Army

USAWC CLASS OF 2001

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

WIELDING THE CYBER SWORD: EXPLOITING THE POWER OF INFORMATION OPERATIONS

by

Lieutenant Colonel Randal A. Dragon
United States Army

Colonel David R. Brooks, USA
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Randal A. Dragon

TITLE: Wielding the Cyber Sword: Exploiting the Power of Information Operations

FORMAT: Strategy Research Project

DATE: 13 March 2001 PAGES: 30 CLASSIFICATION: Unclassified

Information Operations (IO) are rapidly becoming a new Battlefield Operating System (BOS). Until the last 3-5 years, emphasis in applying the tenets of IO remained compartmented discretely within organizations at each level of war – strategic, operational, and tactical. Given the infusion of technology and the potential merger of those levels, information has become a currency for all operations across the spectrum of conflict. With the goal for IO to achieve Information Superiority, this study examines current IO doctrine and organization in light of expectations of the future battlefield and the transformed Army. The fundamental conclusion is that to develop into a viable contributor as a warfighting domain, IO should be formally recognized as a BOS and sub-divided to encompass two types of operations: influence/perception operations focused on the message; and network/cyber operations focused on the media. In the final analysis, current IO systems require radical modification with respect to doctrine, organization, leader development, and training.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

WIELDING THE CYBER SWORD: EXPLOITING THE POWER OF INFORMATION OPERATIONS

> "The military establishment must acknowledge that the face of battle is changing. Information, as a dimension of conflict and competition, has vaulted to the forefront of importance of the future national security landscape and now must rank as at least co-equal with air, ground, sea and space dimensions. Yet, even with its importance, we have just begun the intellectual examinations necessary to develop a viable theory of IO that will underpin any discussion of war in the digital age."[1]

Information leads to knowledge, and knowledge to power. With the advent of the Information Age, the nature of military operations changed forever. Battlefields dominated by mass are yielding to ones of precision – precise firepower supporting precise maneuver enabled by precise information. The Post-Cold War security environment created a number of diverse challenges, but the general maxims of success have not changed: the combatant that develops and sustains military potential – trained, manned, equipped, and ready – and is willing to decisively apply that potential emerges the victor. This study addresses a significant wellspring of the new security environment – the emergence of Information Operations (IO).

The study methodology analyzes current and future contingency environments and identifies why the future force will need to integrate information across the spectrum of conflict (peace to major theater war). After reviewing the information environment, the study defines some of the implications on IO caused by a more complex environment. An overview of current IO doctrine highlights the diversity of IO tools that a Joint Force Commander (JFC) must integrate. Additionally, a description of the future battlespace, the overarching concepts from Joint Vision 2020, and the key concepts from the Army's vision point to several unique demands and capabilities required from future IO systems. Finally, the author recommends areas where Information Operations can be better integrated, making it a more responsive tool at the national, theater strategic, operational, and tactical levels.

BACKGROUND

The concept of using IO is nothing new. During Desert Shield and Desert Storm, employment of offensive and defensive IO sustained the Coalition and negated Saddam Hussein's strategy. Hussein's attempts to intimidate neighboring countries with SCUDs, his threat to inflict massive casualties, and his efforts to rally fellow Arab nations around Iraq for the sake of Arab unity failed due to Coalition defensive IO measures. In addition, Coalition forces successfully applied deception and Operations Security (OPSEC) to fix Iraqi forces in place while hiding their intent to maneuver and attack Iraqi weakness. The use of a sound information

strategy throughout this campaign ensured Coalition success and never allowed Iraq to gain the initiative.[2]

In Somalia, the use of information worked against the United States' strategy. When a UH-60 helicopter was shot down, and an alert news crew captured the images of dead U.S. Army Rangers being dragged through the streets of downtown Mogadishu, a major shift in U.S. policy occurred within 24 hours.[3] A relatively unsophisticated adversary waged this information campaign against a technologically advanced society. "The loss of eighteen rangers in close, back alley fighting in Somalia dramatically underscored a corollary of (General William) DePuy's maxim: a tactical engagement fought for too high a price for too little return might very well by itself determine the strategic outcome of a national endeavor."[4]

The most recent campaign, the conflict in Kosovo, demonstrates the power of combining the Internet and the media. Both sides achieved the information upper hand for short periods and influenced popular perception and, as a result, influenced key decision-makers. According to the Los Angeles Times, the Kosovo conflict turned "cyberspace into an ethereal war zone where the battle for the hearts and minds (was) being waged through the use of electronic images, online discussion group postings, and hacking attacks."[5] The Kosovo conflict was characterized as the "first war on the internet. Government and non-government actors alike used the net to disseminate information, spread propaganda, demonize opponents, and solicit support for their positions ... and people everywhere used it to discuss the issues and share text, images, and video clips that were not available through other media."[6]

Rapid growth of the Information Technology industry has fueled changes within the armed forces and led to what some have called a "Revolution of Military Affairs." The Army's change, dubbed the Army Transformation, represents not only the physical arming and re-structuring of the force, but also a window of opportunity to integrate all available tools and allow the force to deploy faster, fight with unprecedented speed and lethality, and win decisively. With proposed changes, the Army will move from the Industrial Age to the Information Age providing an Army with immense capability in terms of relative speed, flexibility, versatility, adaptability, and precision.[7] The Information Age Army changes the architecture (deep, close, rear) of the battlefield and alters the accepted levels of war framework (strategic, operational, tactical). Now, more than ever, it appears that integrating information into our strategy, campaigns, and tactical plans will be the true impetus to success.

Intertwined with this transformation is an opportunity to capitalize on our ability to influence, both through the threat of combat power, and through the management of others' perception. Without a true peer competitor on the near-term horizon, we have an opportunity to

strengthen our employment of all elements of national power (political, economic, military, informational) to avert potential crisis. The use of information cannot be exclusive to our national strategy. Indeed, for continuous success, every echelon of leadership and command must have the tools and the know-how to integrate information. In layman's terms, the goal of an information operation is to keep an adversary or potential enemy from doing what we don't want him to do, or to stop him from doing something that he is doing. To be effective, IO must be fully integrated and synchronized, from national through operational level, to achieve the desired effect.

CURRENT ENVIRONMENT

The information environment provides a pool within which all other relevant infrastructure subsets operate. As defined, "the information environment is the aggregate of individuals, organizations, or systems that collect, process, or disseminate information, including the information itself."[8] Relevant to this research are three information infrastructures shown relationally in Figure 1: Global (GII), National (NII), and Defense (DII).

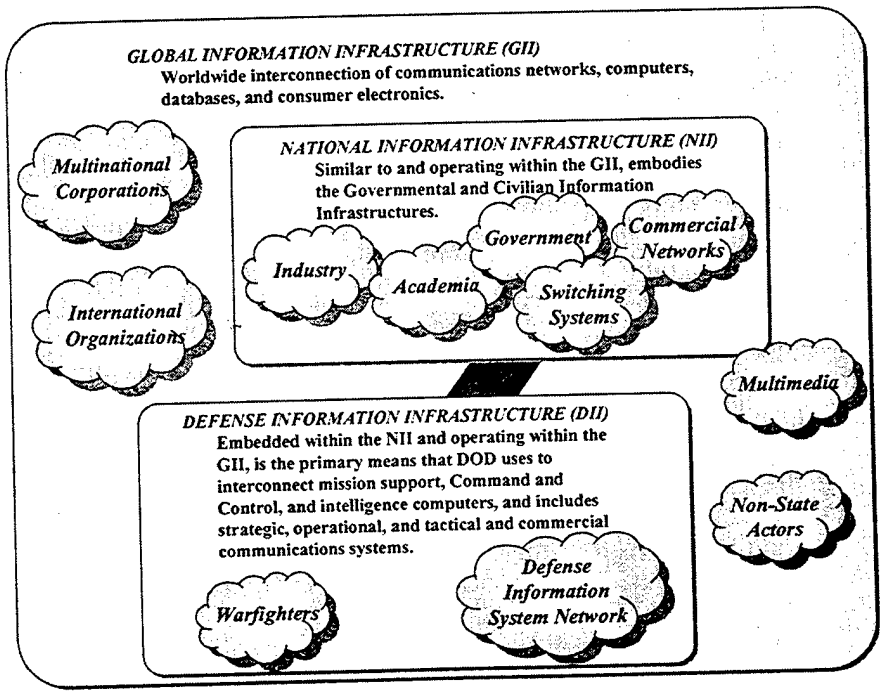

FIGURE 1. INFORMATION ENVIRONMENT[9]

Like these information environments, IO includes hardware, but is <u>not</u> hardware-centric. The current joint definition states that IO are "actions taken to affect adversary information and information systems while defending one's own information and information systems."[10] It goes

on to characterize IO "as targeting information or information systems in order to affect the information-based process, whether human or automated."[11] The GII is the domain in which we conduct IO, with the informational element of national power emanating from the NII, and Information Operations generated from within the DII.

Embedded within all of these definitions is the term "information," defined "as facts, data, or instructions in any medium or form. It is the meaning that a human assigns to data by means of the known conventions used in their representations."[12] Data is normally sensed, reported, arranged, and processed. Once processed, these data become information and, with cognition, the information becomes knowledge. To influence or alter an adversary's perception, joint operations employ both offensive and defensive capabilities. The fundamentals of offensive IO, which can best be described as "perception management," are as indicated in Figure 2.

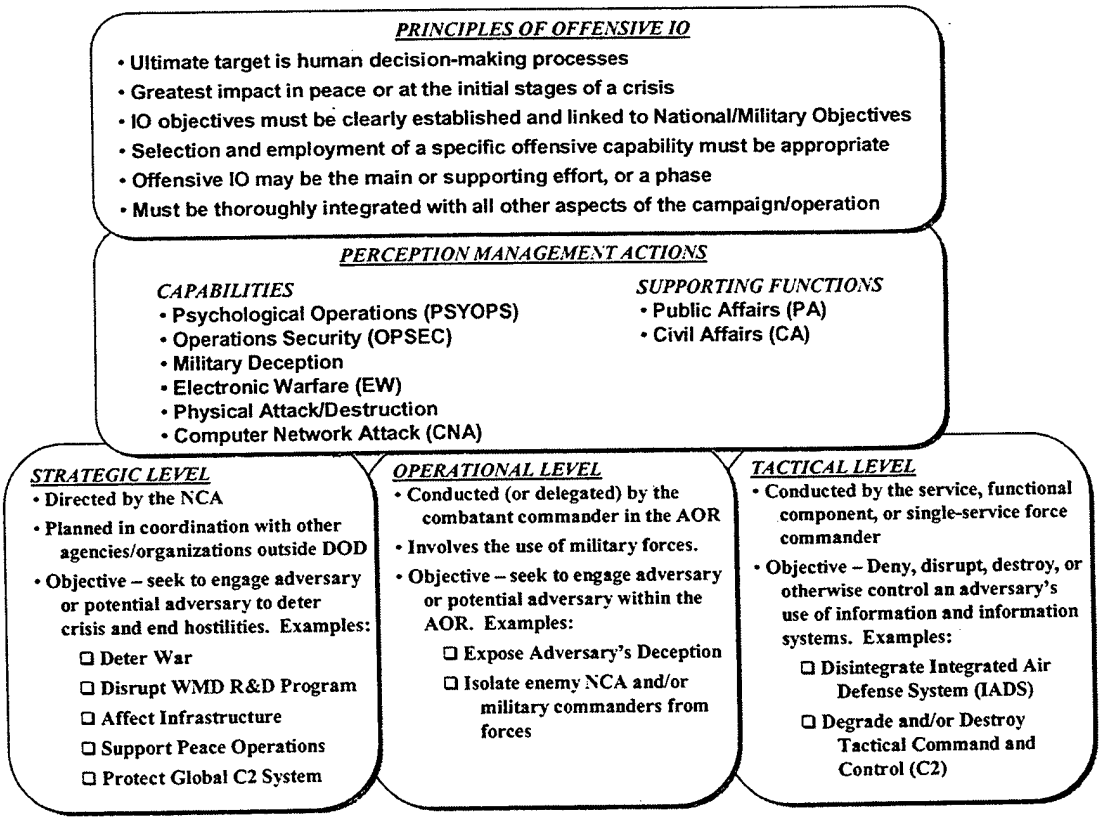

FIGURE 2. OFFENSIVE IO FUNDAMENTALS[13]

Defensive IO is similar in scope to offensive, however its emphasis is on defending and protecting friendly information and information systems. These operations are conducted through Information Assurance (IA), Information Security (INFOSEC), Physical Security,

Counterdeception, Counterpropaganda, Counterintelligence (CI), Electronic Warfare (EW), and Special Information Operations (SIO).[14] Integration of offensive IO with defensive IO is essential, as is the integration of IO with the other aspects of operations (maneuver, fires, reconnaissance, etc.).

From the Army's standpoint, information is a tool which, when leveraged with other elements of power and integrated with other operating systems, can set and sustain conditions that lead to decisive results. Given current definitions, IO encompasses everything short of physical symmetrical combat. For comparison purposes, the Army defines IO as "actions taken to affect adversary, *and influence others' decision-making processes*, information and information systems while protecting one's own information and information systems."[15] This differs from the joint definition (italics above) emphasizing that the effort also targets the decision-making process, and adding the phrase "and influence others'" to account for indirect supporters of an adversary and non-state actors. As a target for IO, the decision-making process is both continuous and dynamic. For discussion purposes, Figure 3 shows two command and control (C2) process models with embedded decision-making.

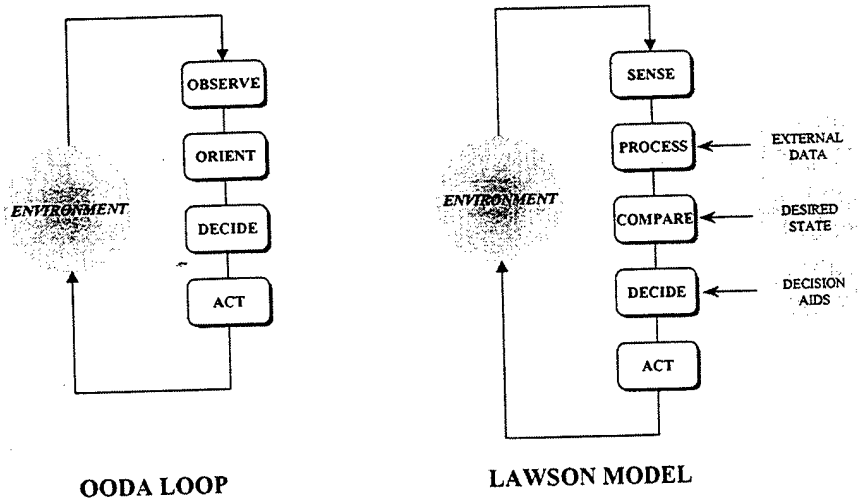

FIGURE 3. C2 PROCESS MODELS[16]

The OODA Loop is a simple C2 model best suited to model tactical combat engagement decisions (trigger pulling). IO affects the entire process, but would specifically focus on what and how an adversary (or other) observes something within the environment. Therefore, the main IO effort would focus on altering the environment or influencing the OBSERVE function. In Lawson's model, IO not only affects the environment and the SENSE function, but might also be

used to disrupt, deny, or alter EXTERNAL DATA or DECISION AIDS, or may change the perception so that the DESIRED STATE is corrupted. Regardless of the model, the impact of IO is its affect on the decision-making process.

VISION OF THE FUTURE FORCE

Joint Vision 2020 (JV2020) embodies the overarching concepts that guide future joint force development. More descriptive than prescriptive, it portrays an environment of faster, more lethal, and more precise application of military power to meet national security requirements. The heart of JV2020 is the concept of Full Spectrum Dominance, which "implies that U.S. forces are able to conduct prompt, sustained, and synchronized operations with combinations of forces tailored to specific situations and with access and freedom to operate in all domains – space, sea, land, air, and information."[17] Information is so critical to success in the future that it has been explicitly listed as a warfighting domain. Given these domains, how many potential offensive and defensive pairings must the Joint Force Commander (JFC) account for?

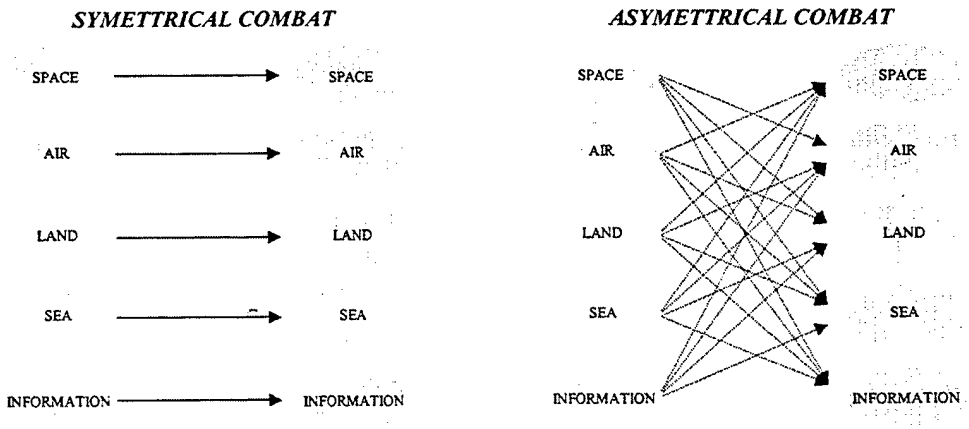

FIGURE 4. WARFIGHTING DOMAINS

Symmetrical combat, though undeniably important, may become less significant for the JFC, with asymmetrical combat and counter-asymmetrical defense mechanisms becoming the issue.[18] Assuming symmetrical combat shown in Figure 4 (i.e. land vs. land, air vs. air), the JFC must plan and execute in 5 offensive dimensions of combat. Assuming asymmetrical combat (i.e. air vs. land, land vs. air), the challenge expands to directing and controlling 20 possible offensive dimensions, and 25 when including symmetrical combat. If the adversary has similar

combat potential, the defensive challenge is now 25 separate threats, all which could conceivably be employed in combination.

Full Spectrum Dominance depends on Information Superiority – that is, "the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[19] Information alone is insignificant unless we can translate the information into knowledge and decisions – decisions that are faster, better, and more precise. Decisions that enable our forces to strike precisely, maneuver with impunity, and paralyze an enemy through its sheer speed and essence of uncertainty. Within an asymmetrical framework, it becomes clear that information enables the other functional areas, affording the JFC positional advantage and an ability "to employ decisive combat power that will compel an adversary to react from a position of disadvantage, or quit."[20]

The supporting Army vision describes a transformed force possessing increased strategic responsiveness and tactical staying power. Designed to operate as part of a joint, combined, or multinational formation across the spectrum ranging from peacekeeping to Major Theater War (MTW), the transformed Army "will provide the Nation an array of deployable, agile, versatile, lethal, survivable, and sustainable formations, which are affordable and capable of reversing the conditions of human suffering rapidly and resolving conflicts decisively."[21] The underlying premise of the transformed force is to transport decisive landpower to a theater of war to prevent or preclude combat. Should combat be necessary, the force must engage with precision fires and maneuver to win decisively.[22] Under current roles and responsibilities, the Army's contribution to the joint team remains one focused on fighting and winning the Nation's wars.

VISION OF THE FUTURE BATTLESPACE

Future warfare promises to be more chaotic and complex. It will be driven by both nation-state and rogue/transnational actors who apply symmetrical and/or asymmetrical tools either as force, or the threat of force, creating a mosaic of security requirements. The National Intelligence Council report Global Trends 2015: A Dialogue About the Future with Nongovernment Experts indicates that due to the United States' strong technological lead in battlefield awareness and precision guided weaponry, three types of threats will exist: asymmetric threats, strategic WMD threats, and regional military threats.[23] Asymmetric threats, as described in this context, represent terrorism, sabotage, cyber-crimes, and the like. Martin Libicki, National Defense University, offers similar views and states that as a result, the advent of what he calls the "Global Grid" will support future warfighting in three general categories: (1)

The development of standoff warfare which focuses on destroying an enemy; (2) New coalitions, linked to the grid with common Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR); and (3) The attractiveness of low intensity conflict in a constrictive environment (which he refers to as "mud warfare") as a response to total technological overmatch.[24] Essentially, both Libicki and the National Intelligence Council agree that potential enemies will attempt to negate or mitigate any technological edge and initiate warfare either where the consequences are extremely high, or preferably, in situations where technology proves to have marginal value-added.

As outlined above, the transformed Army will field a versatile force capable of rapid deployment, agile employment, and self-contained staying power. As the opportunity arises in combat, this force will attack operational or strategic centers of gravity (critical force, C2 node, seat of national power, key infrastructure) leading to decisive results. Given these fundamental battlespace conditions, there are several parameters that must be considered in developing "IO-future."

First, all future peer competitors will become increasingly capable and lethal with precision fires causing the battlefield to spread out even further.[25] To preempt this, the transformed force must remain dispersed and outside the operational reach of the enemy, striking rapidly with precise maneuver against the center of gravity when the conditions are right. The current response to this, then, is to increase speed. Scales points out that "the challenge we face is very similar to the challenge that armies have faced for hundreds of years. In order to collapse the enemy's will to resist, we have to cross the deadly zone. We have to be able to get through the enemy's area of effectiveness to strike at his operational center of gravity and collapse it in order to achieve victory."[26] The implications for IO here are threefold: (1) IO (along with the intelligence function) must support pinpointing the attack objective and the avenues that will result in minimal impedance (damage/delay) to the attacking force, (2) IO must disrupt and paralyze the enemy commander leaving him unable to effectively interdict attacking forces, and (3) we must know when commitment conditions are met.

Second, the future environment will encompass the spectrum of conflict ranging from peace to war, but with greater depth, complexity, and consequence than we know today. As a result, the demands placed on IO will increase, with the nature and scope of a specific operation deciding the true mix of IO variables. In peacetime operations, we will engage in IO as a part of a CINC's Theater Engagement Plan (TEP) to shape the environment and meet National Security Strategy goals. Once a crisis erupts, IO system flexibility must enable a shift from proactive (peacetime engagement) to reactive (crisis) while maintaining a sure hand on the

cause-effect history of past IO in the area of operations/area of interest. Additionally, the importance of IO varies with time over the course of an operation. For instance, IO may start as the lead aspect during peacetime engagement (i.e. CINC TEPs) and may continue to remain dominant in the early phases of a crisis, but will take a supporting role to physical operations during conflict, and then return as the lead aspect during the post-hostility phase of an operation as depicted below.

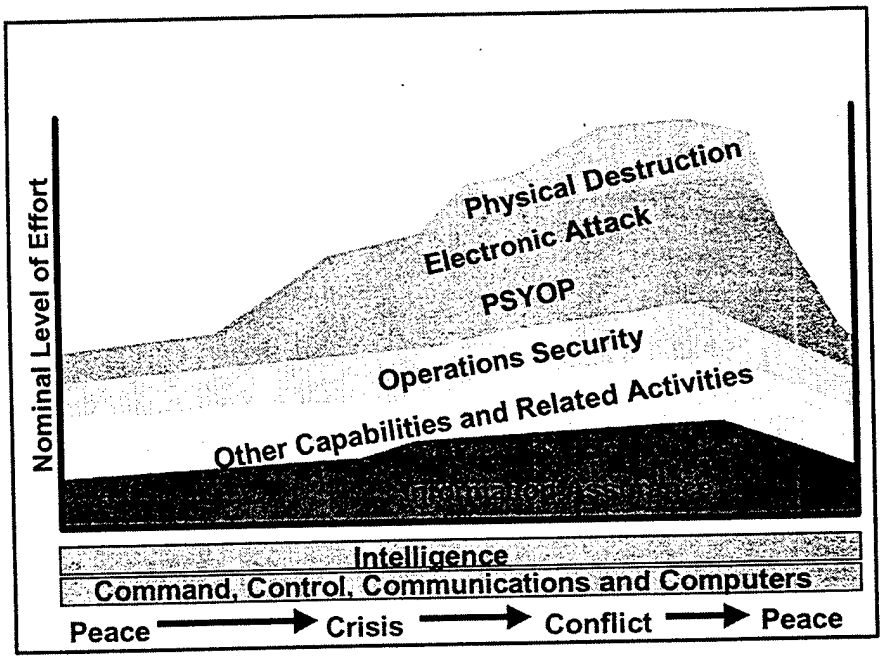

FIGURE 5. NOTIONAL INFORMATION OPERATIONS ENGAGEMENT TIMELINE[27]

The underlying issue is how to organize IO assets to meet functional requirements within a specific operation, while providing consistent and coherent support across the conflict spectrum. The objective system must provide an organization which implements IO equally well over the entire spectrum of potential conflict and ensures information superiority. In other words, the organization must maintain operational agility.

To achieve success in the future, we must confront the enemy with all dimensions simultaneously – land, sea, air, and space. The fifth dimension of combat – information – underpins the synchronization of all others assuming some level of information superiority. This implies that we must be able to perform all C2 information functions (acquire, process, distribute/analyze, protect, and others) with impunity while denying our adversary the same. As

a result, our future systems must treat information and likewise, "operations in information," as a critical component of the Information Age force.

Finally, human factors and human dynamics transcend military operations. There is a limit to the amount of information the human brain can process. The sheer speed of envisaged operations raise the demand for faster C2 processes. Future leaders must direct the movement of units over great distances in short periods of time, orchestrate and manage the enemy's perception (what the enemy sees or thinks he sees), and synchronize maneuver with fires to fix, maneuver, and destroy the enemy – all at a minimum cost. More than ever, the holistic nature of these operations demand changes in how we train and prepare our leaders, how we organize our C2 and IO processes to support the commander, and how we leverage IO in support of dominant maneuver and precision engagement.

CURRENT CHALLENGES IN MEETING FUTURE DEMANDS

To truly make IO a weapon, we must be willing to answer several questions. First, have we changed the way we approach "information" as an entity? An interpretation of the current definition shows that IO includes two virtual sub-systems: (1) operations conducted to influence, persuade, or paralyze a potential adversary, and (2) operations against a supporting system or an information infrastructure to degrade an adversary or potential adversary's C2 ability. Although JV2020 describes information as a fifth domain, current joint doctrine leaves broad latitude for service-specific interpretation and implementation and has evolved to prosecuting IO through loosely affiliated, ad hoc joint organizations.

Second, is our doctrine sufficient to enable synchronization of the information effort? Currently, we use an artillery-centric Decide-Detect-Deliver-Assess model to plan, prepare, coordinate and assess IO.[28] Does this support "information maneuver" and enable identifying centers of gravity, lines of maneuver, and decisive points for information? Will future doctrine drive change to account for: (1) a future information environment that demands better interagency cooperation, and (2) seamless and consistent joint operations across the full spectrum?

Third, every IO has a different response time and a different set of information filters that can (potentially) alter the "sent" message (Figure 6). Additionally, each IO can result in different response or reaction times. With the decision-maker at the center, all other tiers or systems provide information input. Are our techniques sophisticated enough to understand and manipulate these variables and achieve the desired outcome at the intended target? Do we understand the affect of the information filters? Given the human factors and cultural

differences, do we have the appropriate measuring devices and metrics to determine whether we have met our objective?

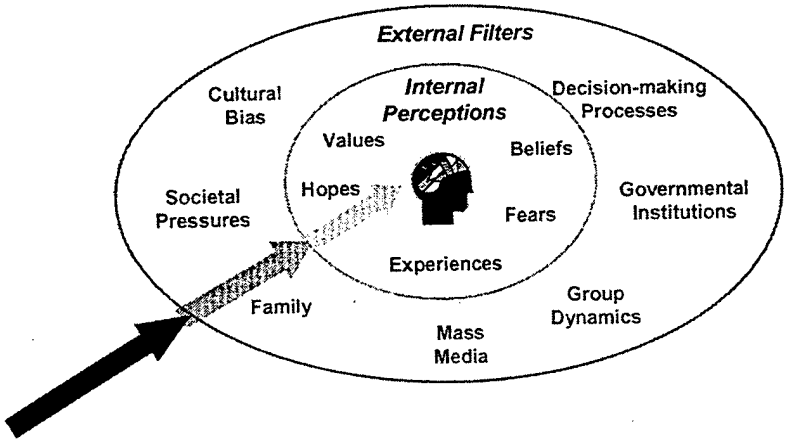

FIGURE 6. PERCEPTION MANAGEMENT[29]

Fourth, cyber-warfare presents unique challenges. Do we really understand the impact of a full-scale cyber-attack? What will the electrons affect, how many intermediate systems will they travel through, and what will be the total impact? When someone launches an arrow in cyberspace, like a virus, we may be able to assess the impact. What happens when that arrow becomes the size of a cyber hand grenade, a cyber artillery round, or a cyber nuclear munition? Will it impact at a specific point, or will it fracture, continue to multiply until what was originally sent with the intent to shut down an adversary's information network, actually results in the alteration of the global positioning data, flood gates on dams being opened, nuclear reactors being affected, or air/rail network information distortion?

Finally, are we structuring our future forces for symmetrical dominance? If so, which of our potential competitors is truly in a position to procure and maintain the quantity and quality of high technology equipment needed to defeat our future force? If our adversary becomes unwilling and/or unable to fight us symmetrically, will we have the defensive protection mechanisms in place to defeat the asymmetrical threat? With respect to information, this means placing due emphasis on protecting infrastructure and information systems.

REACHING FORWARD FOR SOLUTIONS

The integration of IO into future systems is inextricably dependent on the effect of future technology on the levels of war – strategic, operational, and tactical. As information systems become more reliable, the ability to share a common operating picture and achieve battlespace awareness at every level increases. Since information is neutral this can also work against us.

Gen (Ret) John Sheehan, former Commander of U.S. Atlantic Command, emphasized that "new information technologies continue to blur the distinction between tactical, operational and strategic decisions. Thanks to SkyNews and CNN, a young officer's or NCO's decision in the field will be shown to millions around the world."[30] For future operations, our ability to employ offensive IO and protect using defensive IO will be critical to success.

In a historical context and given "typical" circumstances in the need for military intervention, we have fairly well defined roles and responsibilities for strategic, operational, and tactical applications of military force. The National Command Authorities (NCA) establish objectives for the military, forces and resources are organized to meet those objectives, and the forces are then employed. In the atypical environment of IO, the method of deployment and employment are neither overt nor, in most cases, as measurable. As a result, the impact of a deception operation, or the influence of a psychological operation, targeted at the operational level but having significant consequences at the strategic level may have secondary and tertiary effects for all – the lines are blurry and in some cases, the separation meaningless.

In describing future conflict, MacGregor concluded that the "technologically altered battlefield dimensions of time and space will merge the three levels of war into a single new structure for the integration of complex air-land-sea combat operations."[31] The merged levels, enabled by information, will "allow actions at every level to instantaneously affect each other."[32] If an outgrowth of information age warfare is compression of the levels of war, then coordination between all levels emerges as a fundamental necessity to ensure a common theme and consistent results. Since each situation is different, the target must be known, with a clearly defined end state described. The bottom line is that technology and globalization are changing the way that we categorize warfare. More importantly, due to increased situational awareness throughout the force, actions that occur at any level will have an immediate impact at all other levels. The IO system of the future must leverage and account for the offensive and defensive implications of these phenomena in future operations.

INFORMATION OPERATIONS AS AN ENABLER FOR THE TRANSFORMED FORCE

Full Spectrum Dominance implies a force that can dominate every point along the spectrum of conflict. In the future, the force may be required to conduct multiple operations simultaneously at the lower end of the spectrum. As we saw earlier, this implies an IO system that transitions smoothly, from peacetime to contingency support, while remaining coherent from national through tactical levels. It must be equally effective in peace support and major

conflicts, and must provide the supporting commander with the decisive edge with respect to information, and information systems.

Under current design parameters, the transformed Army will deploy a combat Brigade to a contingency theater 96 hours after notification, a Division in 120 hours, and five Divisions in 30 days.[33] To achieve this level of rapid deployment, several information-dependent actions must occur. Deploying forces must leave behind (at least initially) organizations that perform functions that can be done at a distance or those that do not directly contribute to immediate success on the battlefield. This "reach back" reduces transportation requirements and in-theater footprint, thereby decreasing in-theater force protection. During the deployment phase, we need to hold the enemy in check to keep him from doing something that will affect the deployment flow, including both physical nodes (ports of embarkation/debarkation) and electronic nodes (information systems). The force must be capable of rapid assembly, a task enabled by positively influencing the local populace.

The transformed force must be able to engage the enemy with exacting precision at distances that are unfathomable today, while remaining dispersed and outside an adversary's operational reach. This killing range depends on the technological sophistication of the opponent. Coupled with this is a force that must be capable of precise, agile maneuver; actual force speed may well exceed 200 kilometers per hour.[34] This level of speed and precision mandates total knowledge on the enemy and countermeasures to reduce the enemy's knowledge on the friendly force. The technical sophistication of potential enemies will most likely increase. More information will be available, and many times it will be absolutely free and available to anyone who wants it. Decision cycles will be increasingly shorter, and C2 systems will mature to enable real-time transmission of orders. With the compression of levels of war, we may find hierarchical organizations extinct, replaced by fluid architectures. In all cases, to be effective, we must move well inside the enemy's decision cycle, so that he is constantly wondering how the friendly force is doing what it is doing and why they're doing it. As with strike operations, windows of opportunity exist in IO. We must know precisely when and where to apply available IO tools to achieve optimal effects, which means that we must have systems to support that.

The transformed force must be decisive. It must combine all available dimensions to disable an enemy, then deliver a blow that brings conflict to a rapid conclusion and meets the prescribed mission objectives. In order to do this, our information systems must be able to provide relevant information at critical times, while denying the enemy the same. Information superiority increases the enemy's uncertainty and can give friendly forces the ability to achieve

decision superiority. In all cases, IO-future must be tied to national informational efforts, and must leverage the advantage gained by combining the effects of joint assets.

INFORMATION OPERATIONS VECTORS

The Army is at a critical juncture. The transformation will change not only what type of forces we employ, but also how we integrate the resources available to the commander. Now more than any other time in history, information is the critical link for the transformed Army to conduct decisive operations. Given the challenges of the future battlespace and the implications on IO-future, there are critical requirements that must be met with respect to doctrine, organization, training, and leader development.

Doctrine

To stand the test of time, doctrine must be the engine for change. Changing doctrine requires a cultural metamorphosis. We will not inculcate change without changing our mindset: we must prepare to fight in the information domain. We must refrain from thinking about information in a strictly technical sense and treat it more as a true dimension of combat; make it a weapon to be used first as opposed to an entity acknowledged later. In essence, we must raise IO to co-equal battlefield operating system (BOS) status, much like it is considered an element of national power, an element of combat power, and a critical facet of JV2020.

To make IO more "user friendly" for the customer – the joint warfighter – it must be bounded (what is and what is not IO), integrated into every operation, and roles must be defined within the joint community. It can neither remain so broadly defined that it provides no measurable operational impact, nor can it afford to be so amorphous that it is only understood by a highly specialized group of technical specialists. One way to accomplish this is by separating out routine tasks normally performed by the entire force (supporting tasks). Additionally, a joint warfighting IO doctrine must be developed and consistently applied. The doctrine should embody "information maneuver," developed and explained in terms of centers of gravity, objectives, avenues of approach, decision points, with IO-specific phases to an operation/campaign and designed as a "how to fight" doctrine for the information domain, not a catalog of capabilities.

Organization

Sweeping changes are required in how we organize. Since information is another dimension, there may be some benefit in establishing a functional CINC that provides cross-spectrum support, similar to the present day Special Operations Command. Currently, we are

neither postured for peacetime engagement nor able to maintain full time links with national and interagency organizations. Without question, we must streamline our organizations to meet the demands of the uncertain and complex environment anticipated in the future battlespace – an Information Operations Command may help. The objective IO organization should provide a basis for capitalizing on knowledge gained during peacetime engagement, and make us more able to leverage national and interagency efforts. At Army tactical/operational levels this translates to a staff section subordinate to the Operations staff, while consolidating IO "maneuver" units at Corps or higher level. To meet joint contingency requirements, we should investigate the feasibility of establishing Joint Information Operations Task Forces (JIOTFs): scaleable in size, tailorable in scope, and capable of remaining immersed through peacetime engagement. Finally, an empowered CINC-Information could provide the global reach and visibility necessary to accomplish both Computer Network Attack and Computer Network Defense.

Training

In concert with established doctrine, units designed to operate in the information domain must train to fight as a joint team. In addition, we must train our staffs in the nuances of information domain engagements, teaching them to analyze multiple dimensions while educating them on information cause-effect relationships. Our tactical and operational staffs must understand how to adjust priorities/IO avenues of approach based on "information BDA," and should become equally adept at planning lethal and non-lethal uses of force. IO must be fully integrated in training at all Division and Corps-level BCTP exercises, and embedded within joint validation exercises.

Leader Development

Potentially, the biggest challenge is leader development. As we become increasingly reliant on Information Age technology, our leadership must embrace this emergence and provide the energy and vision to exploit information. Senior officers of today, both decision-makers and decision-shapers for Army-future, spent a great deal of their developmental years learning the art of war, operational art, and tactical operations. At some point, we will want our warfighters to have the wherewithal to apply lethal and non-lethal force with equal ease and virtuosity. This requires re-allocating available institutional training time so that we invest an equal amount of time training our leaders to understand and apply doctrine for operations and Information Operations.

Synergy

Taken together, these vectors can provide a substantial edge to U.S. forces. Since future operations promise to engage within a network-centric warfare environment, forward deployed JIOTFs operating under the direction and guidance of the JFC will electronically reach back for much of their support. Decreasing potential exposure reduces the footprint of deployed forces and eliminates some inherent force protection risks in the contested battlespace, further facilitating global maneuver. The JIOTFs, taken from a pool of experts, probably a mix of soldiers, civilian technicians, and social scientists, will provide rapid transition through the full spectrum with established institutional knowledge.

Change will not just happen – Doctrine must lead the way and be the engine. We can ill afford to apply scarce resources and build organizations that neither protect our service members nor set the conditions for decisive operations. Modular, scaleable packages must be routinely integrated, while commanders must have authority/responsibility for IO to influence the direction that they want information to move – this is how true Information Superiority can be achieved.

RECOMMENDATIONS FOR CHANGE

Though IO have been used successfully for quite some time, the methodology and processes for integration are changing. This evolution may require another level of jointness, possibly using information as the basis for a functional CINC: CINC-Information. Additionally, the Army's approach to IO-future cannot be done in isolation; it must also be part of the joint solution. The core mission of the Army must remain to fight and win Nation's wars and, as a result, we can ill afford to bleed off scarce resources designated for killing or kinetic systems to establish the required IO structure. The transformed Army's contribution must complement the joint commander's arsenal.

Doctrinally, we must determine what functions comprise Information Operations. By separating those functions that every unit performs (OPSEC) and eliminating physical destruction, we bound IO to specialization in the non-lethal application of force. A list of potential categories is shown in Figure 7.

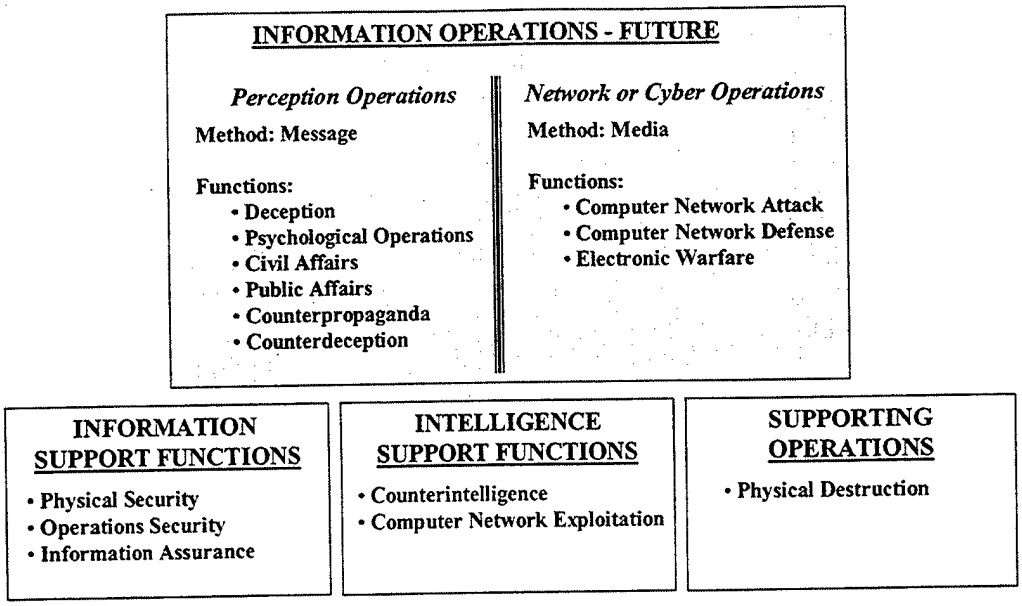

FIGURE 7. DEFINING FUTURE IO FUNCTIONS

Though embedded in a number of lethal and non-lethal systems, information becomes the critical ingredient to the Information Age force. As a result, IO "maneuver" must be developed and deemed as important as operational force maneuver. At the operational and tactical levels this translates to moving IO to BOS-level status. Our doctrine should address how to develop schemes of digital maneuver, aimed at the enemy information centers of gravity, and how to weight the main effort with information – collection, bandwidth, and processing priorities.[35] This system could be supported by digital Integrated Preparation of the Battlefield (or "cyber-prep of the battlefield") and high payoff information targets.

Information Operations must emerge from the cell/committee-based focus and be fully recognized for what it is – another weapon in our arsenal. Once recognized as a BOS and defined by information maneuver doctrine, we need to re-structure our staffs to fully incorporate information. This may require organizations that normally work "directly for the commander" to respond to taskings developed by the Operations Staff, with an embedded IO planner. Likewise, instead of being relegated to a stand-alone cell, lethal and non-lethal plans should be developed by one plans section. Corps and Division-level planners should be equally capable of orchestrating lethal and non-lethal means to mass effects and achieve decisive results.

With respect to organizational structure, we need to evolve, develop, and groom a standing organization – trained, equipped and prepared for deployment – familiar with shared tactics, techniques and procedures (TTP), and keenly aware of the national IO architecture.

This organization, the JIOTF, should have peer status with other lethal and non-lethal combatants, and will frequently be called upon to fully stand up early in crisis. Once deployed, it will be required to provide full IO capability through the post-hostilities phase and well after many of the maneuver forces have returned to homestation.

CONCLUSIONS

The Information Age is not in front of us – we are in it. The future of operations is uncertain; the future of Information Operations is just as uncertain. What is certain is that the battlespace will become increasingly complex. As an institution, we must take proactive steps to modify our toolkit by making our tools operable across the spectrum of conflict. To maintain ascendancy and establish dominance in the future battlespace, our transformed force must integrate every available weapon, the most important of which may be information itself. To achieve decisive results in the information domain, trained leaders must understand the environment, understand and implement a fighting maneuver doctrine for IO, and be able to employ a number of diverse assets across that spectrum. Information leads to knowledge, and knowledge to power. The organization that fully exploits information wields a mighty weapon – the cyber sword.

Word Count = 5,904

ENDNOTES

[1] Wayne M. Hall, "Information Operations: Military Competition," Cyber Sword: The Professional Journal of Joint Information Operations 4, no. 1 (Spring 2000): 6.

[2] Joint Chiefs of Staff, Joint Doctrine for Information Operations, Joint Pub 3-13 (Washington: Joint Staff, 9 October 1998), I-20 – II-3.

[3] Mark Bowden, Black Hawk Down: A Story of Modern War (New York: Atlantic Monthly Press, 1999), 305-313.

[4] Robert H. Scales, Jr., America's Army in Transition: Preparing for War in the Precision Age (Carlisle Barracks: U.S. Army War College, 1999): 20-21.

[5] Ashley Dunn, "Crisis in Yugoslavia – Battle Spilling Over Onto the Internet," Los Angeles Times, 3 April 1999.

[6] Dorothy Denning, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," p.1. Accessed on the internet at <http://www.cs.georgetown.edu/~denning/infosec/nautilus.html.

[7] Department of the Army, "The Army Vision," available from: <http://www.army.mil/armyvision/ armyvis.htm>; Internet; accessed 17 November 2000.

[8] Joint Chiefs of Staff, I-9.

[9] Ibid., I-13 – I-14.

[10] Ibid., I-1.

[11] Ibid., vii.

[12] Ibid., I-9.

[13] Ibid., II-3 – II 14.

[14] Ibid., III-1.

[15] Department of The Army, Information Operations: Doctrine; Tactics, Techniques and Procedures, Field Manual 3-13 (Final Draft) (Washington: U.S. Department of the Army, 30 September 2000), 8.

[16] Kenneth Allard, Command, Control, and the Common Defense (Fort McNair: National Defense University, 1996), 154-156.

[17] Joint Chiefs of Staff, Joint Vision 2020 (Washington: Joint Staff, June 2000), 8.

[18] National Intelligence Council, Global Trends 2015: A Dialogue About the Future With Nongovernment Experts (Washington: Director of Central Intelligence, 13 December 2000), 14.

[19] Joint Chiefs of Staff, Joint Vision 2020, 10.

[20] Ibid.

[21] Department of the Army, 3.

[22] Scales, 24.

[23] National Intelligence Council, 11.

[24] Martin Libicki, Illuminating Tomorrow's War (Fort McNair: National Defense University, October 1999), 31.

[25] Gordon R. Sullivan and James M. Dubik, Envisioning Future Warfare (Fort Leavenworth: U.S. Army Command and General Staff College, 1995), 11-12.

[26] Robert H. Scales, Jr., Future Warfare (Carlisle Barracks: U.S. Army War College, March 2000), 87.

[27] Joint Chiefs of Staff, Joint Doctrine for Information Operations, II-8.

[28] Department of The Army, Information Operations: Doctrine; Tactics, Techniques and Procedures, D-2.

[29] Chris Pilecki, "Information Operations: Joint Pub 3-13 Overview," briefing slides with scripted commentary, Carlisle Barracks, U.S. Army War College, 26 January 2001.

[30] John J. Sheehan, "Building the Right Military for the 21st Century," Strategic Review 25, (Summer 1997): 12.

[31] Douglas A. MacGregor, Future Battle: The Merging Levels of War, Parameters 22 (Winter 1992-1993): 33.

[32] Ibid., 41.

[33] Department of the Army, "The Army Vision," 3.

[34] Scales, 4.

[35] Hall, 8.

BIBLIOGRAPHY

Allard, Kenneth. Command, Control, and the Common Defense. Fort McNair: National Defense University, Institute for National Strategic Studies, 1996.

Allard, Kenneth. Somalia Operations: Lessons Learned. Fort McNair: National Defense University, Institute for National Strategic Studies, January 1995.

Bishop, Roy V. Information Operations: A Layman's Perspective. Strategy Research Project. Carlisle Barracks: U.S. Army War College, 1 April 1997.

Bowden, Mark. Black Hawk Down: A Story of Modern War. New York: Atlantic Monthly Press, 1999.

Clinton, William J. A National Security Strategy for a New Century. Washington: The White House, December 1999.

Copeland, Thomas E., ed. The Information Revolution and National Security. Carlisle Barracks: Strategic Studies Institute, 2000.

Coroalles, Anthony M. "On War in the Information Age: A Conversation with Carl von Clausewitz." Army 46 (May 1996): 24-34.

Denning, Dorothy. "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy," undated. Available from <http://www.cs.georgetown.edu/~denning/infosec/nautilus.html>. Internet. Accessed on 11 September 2000.

Doyle, Kevin J. Information Operations: A Look at Emerging Army Doctrine and its Operational Implications. Fort Leavenworth: U.S. Army Command and General Staff College, School of Advanced Military Studies, 1995.

Dunn, Ashley. "Crisis in Yugoslavia – Battle Spilling Over Onto the Internet." Los Angeles Times, 3 April 1999.

"The Future of Warfare: Select Enemy. Delete." Economist 342 (8 March 1997): 21-24.

Gaston, James C. Grand Strategy and the Decisionmaking Process. Washington: National Defense University Press, 1992.

Grange, David L., and James Kelley. "Information Operations for the Ground Commander." Military Review 77 (March-April 1997): 5-12.

Hall, Wayne M. "Information Operations (IO): Military Competition." Cyber Sword: The Professional Journal of Joint Information Operations 4, No. 1 (Spring 2000): 6-10.

Libicki, Martin C. Illuminating Tomorrow's War. Washington: National Defense University, Institute for National Strategic Studies, 1999.

MacGregor, Douglas A. "Future Battle: The Merging Levels of War." Parameters 22 (Winter 1992-1993): 33-47.

Metz, Steven. Armed Conflict in the 21st Century: The Information Revolution and Post-Modern Warfare. Carlisle Barracks: U.S. Army War College, Strategic Studies Institute, 2000.

National Intelligence Council. Global Trends 2015: A Dialogue About the Future With Nongovernment Experts. Washington: Director of Central Intelligence, 13 December 2000.

Pilecki, Chris. "Information Operations: Joint Pub 3-13 Overview." Briefing slides with scripted commentary. Carlisle Barracks: U.S. Army War College, 26 January 2001.

Scales, Robert H., Jr. Future Warfare. Carlisle Barracks: U.S. Army War College, 1999.

Sheehan, John J. "Building the Right Military for the 21st Century." Strategic Review 25 (Summer 1997): 5-13.

Sullivan, Gordon R., and James M. Dubik. Envisioning Future Warfare. Fort Leavenworth: U.S. Army Command and General Staff College Press, 1995.

U.S. Department of the Army. "The Army Vision" undated. Available from <http://www.army.mil/armyvision/ armyvis.htm>. Internet. Accessed 17 November 2000.

U.S. Department of The Army, Information Operations: Doctrine; Tactics, Techniques and Procedures. Field Manual 3-13 (Final Draft). Washington: U.S. Department of the Army, 30 September 2000.

U.S. Department of the Army. Information Operations. Field Manual 100-6. Washington: U.S. Department of the Army, August 1996.

U.S. Joint Chiefs of Staff. Joint Vision 2020. Washington: Joint Staff, June 2000.

U.S. Joint Chiefs of Staff. Joint Doctrine for Information Operations. Joint Pub 3-13. Washington: Joint Staff, 9 October 1998.

U.S. Joint Chiefs of Staff. Joint Doctrine for Command and Control Warfare (C2W). Joint Pub 3-13.1. Washington: Joint Staff, 7 February 1996.

U.S. National Defense Panel. Transforming Defense: National Security in the 21st Century. Washington: National Defense Panel, December 1997.